FCPED/142/26
April 21, 2026

To: All Microfinance Institutions
Where they are located

Subject: Instruction on Customer Fraud Awareness Campaign

Dear Sir/Madam,

While the adoption of digital financial services has grown significantly in Ethiopia, it has also increased consumer protection risks. Recent incidents indicate a rise in scams and attempted fraud conducted through hacked or impersonated messaging and social media accounts. For instance, Fraudsters are increasingly using platforms such as WhatsApp, Telegram, Facebook, email, SMS and unsolicited or fake phone calls to impersonate individuals and request urgent financial transfers from unsuspecting customers. These schemes pose a growing risk to consumers and may undermine public confidence in digital financial services.

As you are aware, the National Bank of Ethiopia (NBE) is mandated to regulate financial education under Article 6(28) of the National Bank of Ethiopia Proclamation No. 1359/2025. In addition, financial institutions are required to inform customers about fraud risks and their responsibilities in safeguarding financial instruments, as stipulated under Articles 5.1.7 and 5.2.8 of Financial Consumer Protection Directive No. FCP/01/2020.

Accordingly, the National Bank of Ethiopia hereby instructs Microfinance Institutions to implement a customer fraud awareness campaign using appropriate physical communication channels.:

1. **Customer Fraud Awareness Measures**
   1.1. Microfinance Institutions shall display fraud awareness messages through banners and posters within branch premises and other customer service areas. The messages shall be updated and displayed monthly.

   1.2. Microfinance Institutions should prepare and distribute printed leaflets containing fraud awareness messages to customers monthly. Leaflets shall be provided to customers during service interactions and outreach activities.

2. Contents of messages

2.1. Customers should not send money based solely on requests received through social media or messaging platforms such as WhatsApp, Telegram, Facebook, email, SMS or unsolicited phone calls. Customers should verify any financial request through direct voice communication or official contact channels of the purported sender before initiating any transaction.

2.2. Customers must never share PINs, passwords, OTPs, verification codes, or other security credentials with any person under any circumstances.

2.3. Customers should not open suspicious links received through SMS, emails or social media and should only download mobile banking and mobile money applications from trusted sources.

2.4. Customers should regularly check their account or wallet balances and transaction history.

2.5. Customers should not allow strangers or unauthorized individuals to assist them when using ATMs, mobile money and mobile banking applications, or other digital financial services.

2.6. Customers should immediately notify their financial institution if their phone, SIM card, or any device linked to financial services is lost, stolen, or compromised.

2.7. Customers should be encouraged to promptly report any fraud incidents or suspected fraudulent activity related to their accounts to their financial institution through official communication channels.

3. Language and Accessibility

3.1. Messages shall be clear, concise, and easily understandable and Institutions shall ensure dissemination in appropriate local languages to maximize outreach.

4. Fraud Mobile Number Identification and Reporting

4.1. Microfinance Institutions are encouraged are encouraged to identify and take appropriate action on phone numbers and accounts associated with fraudulent activities, including scam messages, fraudulent calls, and impersonation attempts.

4.2. Such cases shall be reported to relevant stakeholders, including Mobile Network Operators, other Microfinance Institutions, Banks and Payment Instrument Issuers and law enforcement and security agencies.

4.3. Any action taken shall be following applicable laws and due process requirements.

5. **Reporting Requirements**

5.1. Microfinance Institutions shall submit a report to the National Bank of Ethiopia monthly, with in Ten (10) days after each monthly campaign in the format attached with this letter

5.2. Compliance with this instruction shall form part of institutions' consumer protection and fraud risk management obligations. Failure to comply may result in appropriate supervisory or corrective actions by the National Bank of Ethiopia.

Sincerely,

Muhidin Shifa
Director, Financial Consumer Protection and Education Directorate

CC:

- **H.E. The Governor**
- **Chief Financial Market and Operations Officer**
  National Bank of Ethiopia

Annex I: Reporting Template for Fraud Awareness Messaging

Channel	**Message Type**	**Number of Customers Reached**			**Observed Fraud Incidents**	**Customer Responses**	**Trend in Fraud Incidents**
		Male	Female	Total			
Banners							
Leaflets							
Others (Specify)							

A) Report Prepared By:
Name:.....Position:.....
Date:.....Signature:.....Mobile/phone:.....

B) Report Approved By:
Name:.....Position:.....
Date:.....Signature:.....Mobile/phone:.....